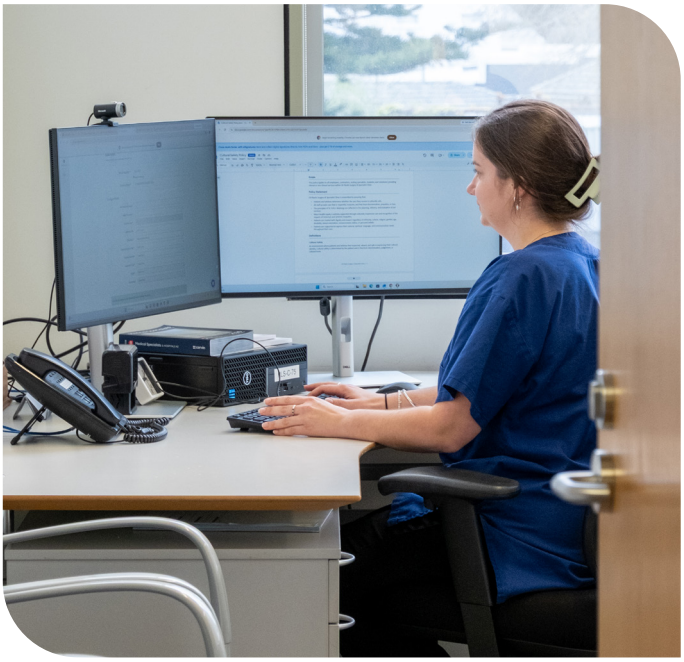
FUJIFILM | codeblue IT services

Success Stories

Building cyber resilience and board confidence at Boulcott Hospital



Boulcott Hospital

Industry
Healthcare

Stronger cyber resilience

Improved visibility, governance and protection across the organisation.

Improved operational efficiency

Modern systems support secure access and flexible ways of working.

Greater board confidence

Regular reporting and clear risk visibility support informed decision-making.

Background

At Boulcott Hospital, delivering high-quality patient care relies on secure, reliable technology, and strong governance.

As healthcare organisations become increasingly dependent on digital systems, Boulcott Hospital recognised an opportunity to strengthen its technology environment, improve cyber resilience, and provide greater visibility of cyber risk for leadership and the Board.

Working with FUJIFILM CodeBlue, the hospital embarked on a programme to modernise its IT environment, strengthen security controls, and establish a more structured approach to managing cyber risk.

"Without secure information systems, you can't run your business."

Graham Dyer | CEO | Boulcott Hospital

Situation

Healthcare organisations manage highly sensitive information and are increasingly expected to demonstrate strong cyber security practices, not only to protect patient data but also to maintain trust and business continuity.

For Boulcott Hospital, the focus was broader than technology alone. Leadership wanted greater confidence that systems, processes and governance arrangements were aligned with the organisation's commitment to patient privacy and operational excellence.

At the same time, the Board was placing greater focus on cyber security and risk management, creating the need for more meaningful reporting and visibility into the organisation's cyber posture.

As cyber threats continued to evolve, Boulcott Hospital recognised the importance of taking a structured approach to understanding and managing cyber risk.

As Graham Dyer, CEO, Boulcott Hospital, explains: "People trust us when they come in here. We're anaesthetising them and operating on them while they're asleep. There's got to be a high level of trust, and that has to extend to everything we do."

Solution

Working alongside Boulcott Hospital, the CodeBlue team helped modernise the hospital's technology environment while strengthening its security and governance capabilities.

The programme included infrastructure upgrades, improved wireless connectivity, enhanced security controls, secure remote access capabilities and the introduction of multi-factor authentication and individual user access controls.

Alongside these technical improvements, CodeBlue conducted a structured cyber risk assessment using its RiskAware framework, helping leadership understand risk exposure, identify priority areas for improvement and establish ongoing governance reporting.

Today, CodeBlue provides managed IT and cyber security services to Boulcott Hospital, combining on-site support with a wider team of specialists to ensure systems remain secure, reliable and well supported.

For Graham, that partnership provides peace of mind.

"It's something we don't need to worry about, because there's someone responsive at the end of the line."

Results

Boulcott Hospital now benefits from a more modern, secure and resilient technology environment.

Staff can securely access systems when working on-site or remotely, while improved infrastructure and support services help keep day-to-day operations running smoothly.



More importantly, leadership and the Board now have greater visibility into cyber risk and a clearer framework for managing it. Cyber security has become a standing item at Board meetings, supported by regular reporting that enables informed discussion and decision-making.

The organisation has also strengthened its cyber maturity through a more structured approach to risk identification, monitoring and remediation.

For Boulcott Hospital, the outcome is not simply stronger technology. It is greater confidence that the organisation is protecting patient information, supporting business continuity and continuing to earn the trust placed in it by patients, clinicians and staff. It also means the hospital is better positioned to meet evolving cyber security expectations across the healthcare sector, with greater visibility of risk and stronger governance processes in place.



"It's a very strong partnership that's based on competency, a shared understanding of needs, and the ability to work together to get things done."

Graham Dyer | CEO | Boulcott Hospital

FUJIFILM | codeblue IT services

Ready to work **smarter?**

Get in touch with the team today.

codeblue.co.nz

0508 48 73 78